



The Latest Scams Circulating the Consumer World.



SEPTEMBER 2011

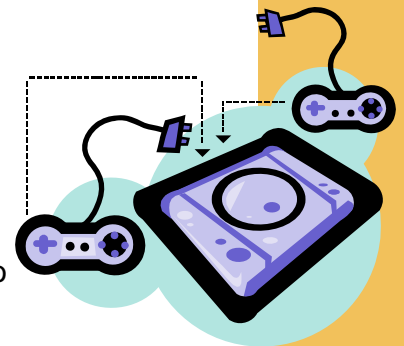
## ONLINE VIDEO GAMES CAN BE IDENTITY THEFT HOT SPOTS

### The Hook

Before playing a video game through the internet, one must first pay to play by entering credit card information online. Many people don't give this a second thought, but those who purchase online are vulnerable to identity theft.

### The Whole Story

Sony Corporation recently acknowledged that its PlayStation network database had been hacked subjecting 77 million of its loyal customers to the theft of their names, addresses, email addresses, birth dates and possibly credit card information. On April 20, 2011 the company shut down its PlayStation Network when it got confirmation of an intrusion on April 16 and 17. Sony has advised its customers to keep a close eye on their credit card statements to ensure there are no unauthorized charges, as well as to change password information. Even though Sony's PlayStation Network is back up and running, it is not 100 percent secure. In fact, all websites in which you input any of your information can be compromised at any time. For more information about the PlayStation hacking, please visit <http://arstechnica.com/gaming/news/2011/04/sonys-black-eye-is-a-pr-problem-not-a-legal-one.ars> and <http://www.redmondpie.com/sonys-playstation-network-is-still-not-safe-should-be-kept-offline-says-expert/>.



### The Lesson

Even huge multinational corporations are not immune to cyber attacks. Anytime information is given out over the internet there is a risk that it could be compromised. To help prevent you from becoming an online identity theft victim, follow these five general tips:

1. Limit any personal financial information you give over the internet. If you want to continue playing online games, or any purchasing transactions online, try buying pre-paid credit cards with limited amounts (some gaming networks only accept certain pre-paid cards - for example, the PlayStation Network [PSN] only accepts PSN pre-paid cards). This way, if your credit card information is stolen you would only be out the amount that is on the card.
2. Be conscious of the risks when you give out your name, address, telephone number, email address, and credit card information. Be extra aware if you must give out your social security number and/or bank account numbers.
3. If you must input your card information online, it is best to use a credit card versus a debit card. With credit card fraud, you have at least 30 days to catch it when you review your statement; whereas with debit card fraud, you generally can't unwind the transaction.
4. Continuously monitor your credit card statements for unauthorized transactions. If you notice any suspicious activity, report it immediately and close your credit card account.
5. Check your credit report annually. Report any mistakes as quickly as possible.